



Homeland
Security

Daily Open Source Infrastructure Report

15 October 2015

Top Stories.

- The former Chicago Public Schools chief executive officer pleaded guilty October 13 in connection to a scheme to steer more than \$23 million in no-bid contracts to a former employer for \$2.3 million bribes and kickbacks. – *WBBM 2 Chicago* (See item [12](#))
- Officials released a report which found that the Internal Revenue Service was unable to locate 1,300 workstations during its attempt to update its Microsoft software from Windows XP to Windows 7. – *Nextgov* (See item [13](#))
- U.S. and European authorities worked with private cybersecurity organizations to disrupt the activities of the Dridex information-stealing botnet. – *Securityweek* (See item [17](#))
- Approximately 100 children and staff were evacuated from the Boys and Girls club in Nevada October 13 after a construction crew hit a 1-inch gas line while digging out a post, causing a gas leak. – *Reno Gazette-Journal* (See item [24](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

See item [14](#)

Chemical Industry Sector

1. *October 13, Carthage Press* – (Missouri) **Employees evacuated from explosives plant after alarms sound.** Fire officials reported October 13 that employees at the explosive plant Dyno Nobel were evacuated from its Carthage plant after an alarm sounded due to a small fire that was extinguished by the sprinkler system. Production and processes have been shut down until officials find the cause of the incident.
Source: <http://www.carthagepress.com/article/20151013/NEWS/151019618>

Nuclear Reactors, Materials, and Waste Sector

2. *October 14, Associated Press* – (Connecticut) **U.S. regulators inspect Millstone over leaking valve.** The U.S. Nuclear Regulatory Commission will continue to conduct an inspection at Dominion Resources Inc., owned-Millstone Unit 2 nuclear power plant October 13 to review issues related to an October 4 incident in which a reactor coolant system leak was linked to a relief valve on the shutdown cooling system at its Hartford plant.
Source: <http://connecticut.cbslocal.com/2015/10/14/u-s-regulators-inspect-millstone-over-leaking-valve/>

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *October 14, Springfield Republican* – (Massachusetts) **ATM ‘skimmer’ admits ripping off \$121,000 from TD Bank customers in 5 Western Massachusetts communities.** A Washington resident pleaded guilty October 9 to charges that he and a co-conspirator used ATM skimming devices to steal over \$121,000 from dozens of TD Bank customers in Chicopee, Ludlow, Springfield, Agawam, and East Longmeadow, Massachusetts, in August and September 2014.
Source:
http://www.masslive.com/news/index.ssf/2015/10/atm_skimmer_pleads_guilty_in_s.ht
[ml](#)
4. *October 13, Reuters* – (International) **UBS settles U.S. SEC case over structured notes for \$19.5 mln.** A U.S. Securities and Exchange Commission official announced October 13 that UBS AG will pay \$19.5 million to resolve civil allegations that the

bank misled U.S. retail investors in offering documents for structured notes tied to a proprietary foreign currency index by not revealing index reductions of about 5 percent through bank hedging trades. The bank neither admitted nor denied the charges.

Source: <http://www.reuters.com/article/2015/10/13/sec-ubs-group-idUSL1N12D1BR20151013>

For another story, see item [17](#)

Transportation Systems Sector

5. *October 14, KMGH 7 Denver* – (Colorado) **2,000 gallons of diesel spills from train car in Fort Collins.** A HAZMAT crew worked to contain a spill in Fort Collins October 13 after a train car tank was punctured and leaked about 2,000 gallons of diesel fuel near a busy intersection.

Source: <http://www.thedenverchannel.com/news/local-news/2000-gallons-of-diesel-spills-from-train-car-in-fort-collins>

6. *October 13, Riverside Press-Enterprise* – (California) **Rancho Cucamonga: Couple victimized hundreds in mail theft operation, police say.** A Rancho Cucamonga couple was arrested October 8 for allegedly stealing hundreds of pieces of mail after a month long investigation revealed stolen pieces of mail, homemade mailbox keys, computers and printers used to make fraudulent checks, and dozens of fraudulent checks. The investigation remains ongoing October 13.

Source: <http://www.pe.com/articles/cucamonga-783315-rancho-couple.html>

Food and Agriculture Sector

7. *October 13, U.S. Food and Drug Administration* – (California) **New Frontier Foods, Inc. issues voluntary recall of Ocean's Halo Seaweed Chips produced at third party manufacturer on certain dates, because of possible health risk (undeclared allergen – wheat).** The U.S. Food and Drug Administration reported October 12 that Burlingame, California-based New Frontier Foods, Inc., issued a voluntary recall of its Ocean's Hal Gluten Free Seaweed Chips produced at a third party manufacturer due to an undeclared wheat allergen after routine testing showed levels of gluten above the FDA limit for a gluten free product.

Source: <http://www.fda.gov/Safety/Recalls/ucm466681.htm>

8. *October 13, Fayetteville Observer* – (North Carolina) **Leak forces Tar Heel plant to evacuate.** A Bladen County official reported October 12 that an ammonia leak prompted the evacuation of the Smithfield Pack Co. for several hours while crews ventilated the building after the leak began near the top of the pork processing plant. HAZMAT crews cleaned the scene and no injuries were reported.

Source: http://www.fayobserver.com/news/local/leak-forces-tar-heel-plant-to-evacuate/article_97f8620e-4bd3-5bf1-9f8d-3351e73fee5.html

Water and Wastewater Systems Sector

See item [27](#)

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

9. *October 14, KTBS 3 Shreveport* – (Louisiana) **Evacuation advisory lifted in Bienville-Webster parish wildfires.** Fire crews worked October 14 to contain several wildfires that burned more than 2,900 acres across Louisiana and prompted evacuation orders for dozens of homes. At least four structures were burned in the wildfires.
Source: <http://www.ktbs.com/story/30252954/wildfire-rages-near-webster-bienville-line-sabine-evacuations>
10. *October 14, Mansfield News Journal* – (Ohio) **Bomb threat: Madison evacuates schools.** Madison Local Schools in Mansfield were evacuated and classes were dismissed October 14 due to a bomb threat called into the 9-1-1 center. Officials responded to the threat and are searching the buildings for any suspicious items.
Source: <http://www.mansfieldnewsjournal.com/story/news/2015/10/14/bomb-threat-madison-evacuates-schools/73917934/>
11. *October 14, Delaware County Daily Times* – (Pennsylvania) **Electrical issues force Chester Upland School for the Arts to cancel classes again Wednesday.** Classes at Chester Upland School for the Arts in Chester were closed October 13 – 14 due to a power failure October 12. Utility crews worked to address the issue.
Source: <http://www.delcotimes.com/general-news/20151013/electrical-issues-force-chester-upland-school-for-the-arts-to-cancel-classes-again-wednesday>
12. *October 13, WBBM 2 Chicago* – (Illinois) **Ex-CPS chief pleads guilty to kickback scheme.** The former Chicago Public Schools chief executive officer (CEO) pleaded guilty October 13 to charges in connection to a bribery scheme where the former CEO accepted \$2.3 million in bribes and kickbacks in exchange for SUPES Academy and its owners to receive over \$23 million in no-bid contract dating back to 2013.
Source: <http://chicago.cbslocal.com/2015/10/13/ex-cps-chief-barbara-byrd-bennett-pleads-guilty-to-kickback-scheme/>
13. *October 13, Nextgov* – (National) **IRS can't update woefully out-of-date Windows server because it can't find some of them.** The Treasury Inspector General for Tax Administration at the U.S. Department of the Treasury released a report which found that the Internal Revenue Service was unable to locate 1,300 workstations during its attempt to update its Microsoft software from Windows XP to Windows 7. The report also determined that the bureau had several thousand servers still running Windows Server 2003 and lacked proper oversight, among other security risks.
Source: <http://www.nextgov.com/cio-briefing/2015/10/irs-cant-update-woefully-out->

[date-windows-servers-because-it-cant-find-some-them/122770/](#)

14. *October 13, KVAL 13 Eugene* – (Oregon) **Federal lab evacuated after ‘credible’ bomb threat.** The U.S. Department of Energy-owned National Energy Technology Laboratory in Albany, Oregon, was evacuated for several hours October 13 after receiving a credible bomb threat. Police searched the facility and cleared the scene after nothing suspicious was found.
Source: <http://www.kval.com/news/local/Federal-lab-evacuated-after-credible-bomb-threat-332479702.html>
15. *October 13, KYTV 3 Springfield* – (Missouri) **2 students arrested; superintendent: Map had classrooms circled and labeled bomb, bomb, bomb.** Two students from Ava Middle School in Missouri were arrested October 13 after the school was evacuated and searched following the discovery of a note in the hallway that mapped out the school with markings of bombs and circled classrooms. Classes were dismissed and police cleared the scene after nothing suspicious was found.
Source: http://www.ky3.com/news/local/2-students-arrested-superintendent-map-had-classrooms-circled-and-labeled-bomb-bomb-bomb/21048998_35828424

For another story, see item [20](#)

Emergency Services Sector

16. *October 13, WLUK 11 Green Bay* – (Wisconsin) **Police search for two escapees from Winnebago Correctional Center.** Authorities are searching for two inmates who escaped from the Winnebago Correctional Center in Oshkosh October 9. Officials believe that the men escaped from a fenced area in the yard.
Source: <http://fox11online.com/news/local/fox-cities/oshkosh-police-searching-for-two-escapees-from-winnebago-correctional-center>

Information Technology Sector

17. *October 14, Securityweek* – (International) **Authorities seize servers to disrupt Dridex botnet.** U.S. and European authorities worked with private cybersecurity organizations to disrupt the activities of the Dridex information-stealing botnet by poisoning the peer-to-peer (P2P) network of each sub-botnet, redirecting infected systems’ communications from the botnet to a sinkhole. The botnet resulted in estimated losses of \$10 million in the U.S., and authorities are seeking to extradite one of its administrators who was arrested in Cyprus in August.
Source: <http://www.securityweek.com/authorities-seize-servers-disrupt-dridex-botnet>
18. *October 14, Securityweek* – (International) **Chrome 46 patches vulnerabilities, simplifies page security icon.** Google announced the release of version 46 of its Chrome Web browser, which addresses 24 security vulnerabilities including a cross-origin bypass in the Blink rendering engine, a user-after-free in PDFium and ServiceWorker, and a bad cast issue in PDFium, among others. The update also changed the icon used for Hypertext Transfer Protocol Secure (HTTPS) connections.

Source: <http://www.securityweek.com/chrome-46-patches-vulnerabilities-simplifies-page-security-icon>

19. *October 14, Securityweek* – (International) **Microsoft patches critical flaws in Windows, Internet Explorer.** Microsoft released 6 security bulletins addressing over 30 vulnerabilities, including 14 memory corruption, privilege escalation, information disclosure, VBScript and JavaScript address space layout randomization (ASLR) bypass, and remote code execution flaws in Internet Explorer, as well as other ASLR bypass and remote code execution vulnerabilities in Windows, among other fixes for Edge, Office, and the Windows kernel.
Source: <http://www.securityweek.com/microsoft-patches-critical-flaws-windows-internet-explorer>
20. *October 14, Softpedia* – (International) **Adobe Flash Player zero-days used by hackers linked to Russian government.** Security researchers from Trend Micro warned that attackers in the Operation Pawn Storm cyber-espionage campaign are exploiting unpatched zero-day vulnerabilities in Adobe Flash Player in an effort to trick members of overseas government departments and ministries to access Web sites hosting malicious code. The group previously targeted high-profile government targets worldwide, as well as the North Atlantic Treaty Organization (NATO) and the U.S. White House.
Source: <http://news.softpedia.com/news/adobe-flash-player-zero-days-used-by-hackers-linked-to-russian-government-494509.shtml>
21. *October 13, Securityweek* – (International) **Adobe patches many flaws in Flash Player, Acrobat, Reader.** Adobe released updates addressing 56 vulnerabilities in Adobe Acrobat Reader, many of which involve bypass restrictions on JavaScript Application Program Interface (API) execution and bypass vulnerabilities that could lead to information disclosure, memory leak issues, and memory corruption bugs, resulting in remote code execution, as well as 13 use-after-free, buffer overflow, memory corruption, and same-origin-policy (SOP) flaws in Flash Player, among others
Source: <http://www.securityweek.com/adobe-patches-many-flaws-flash-player-acrobat-reader>
22. *October 13, Threatpost* – (International) **Netgear publishes patched firmware for routers under attack.** Netgear published firmware updates addressing a remotely exploitable authentication bypass vulnerability that hackers had exploited to take over up to 10,000 routers, most of which were in the U.S. The flaw allowed an attacker to access the device's administration interface without knowing the router password.
Source: <https://threatpost.com/netgear-publishes-patched-firmware-for-routers-under-attack/115006/>

For another story, see item [13](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

Communications Sector

Nothing to report

Commercial Facilities Sector

23. *October 13, New York Daily News* – (New York) **Possibly dangerous flaw found in 60 NYC buildings' elevators.** The Department of Buildings issued a warning October 12 requiring owners of a specific brand of elevators found in 60 buildings across New York City, to operate the lifts manually or shut down the elevators after an October 2 accident killed a man while trying to escape a stalled elevator. Owners of the affected buildings have been advised to hire their own independent inspector to certify the safety of the machines.

Source: <http://www.msn.com/en-us/news/us/possibly-dangerous-flaw-found-in-60-nyc-buildings-elevators/ar-AAfnZPg>

24. *October 13, Reno Gazette-Journal* – (Nevada) **Boys & Girls club evacuated after gas leak.** Approximately 100 children and staff were evacuated from the Boys and Girls club in Reno, Nevada, October 13 after a construction crew hit a 1-inch gas line while digging out a post, causing a gas leak. NV Energy crews shut off gas valves for about 4 to 5 buildings while crews took readings around and inside buildings.

Source: <http://www.rgj.com/story/news/2015/10/13/boys-girls-club-evacuated-after-gas-leak/73869036/>

25. *October 13, KTVI 2 St. Louis* – (California) **Fire at San Leandro Walmart prompts evacuation.** California police arrested a man October 13 on charges for suspicion of arson after allegedly setting an isle on fire in a San Leandro Walmart in which video footage reveals the man leaked a 2-liter bottle of charcoal lighter fluid around the store, prompting shoppers to evacuate for nearly 4 hours. The store reopened, but several isles remained closed.

Source: <http://www.ktvu.com/news/32846443-story>

Dams Sector

26. *October 14, Associated Press* – (Pennsylvania) **State officials to drain 2 northern Pennsylvania ponds, citing weak dams and no funds.** The Pennsylvania Department of Environment Protection and the Fish and Boat commission plan to drain two ponds in northern Pennsylvania after State inspections found the dams at both White Oak and Miller ponds in Wayne County may be a potential hazard if flooding caused them to fail, and officials reported there were no funds to repair the weak dams.

Source:

<http://www.therepublic.com/view/story/78c2bbc98a9a4b36b64cb639cbb0c604/PA--Ponds-Drained-Wayne-County>

27. *October 13, WIS 10 Columbia* – (South Carolina) **City manager: Dam completed at Columbia Canal.** Columbia city officials announced October 13 that the temporary dam built to divert water fully into the Columbia Canal was completed and that a permanent repair could take six months to one year to complete.

Source: <http://www.wistv.com/story/30242434/clean-up-repair-continues-at-columbia-canal>



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.